68. We are adopting a requirement to submit a high level software operational description or flow diagram. The requirement we are adopting is analogous to the requirements in the rules that were developed for hardware based equipment that require applicants for equipment certification to supply a block diagram, schematic diagram and a brief description of the circuit functions of a device, along with a statement describing how the device operates.[105] In this regard, the software operational description or flow diagram must describe or show how the RF functions in the radio, including the modulation type, operating frequency and power level are controlled or modified by software, and must describe the security or authentication methods that are incorporated to prevent unauthorized software changes. The description can include text, logic or flow diagrams, state descriptions[106] or other material that provides the Commission's staff with a reasonable understanding of the operation of a device being certified and whether the device complies with the rules. The Commission's staff will work with applicants for certification to ensure that these requirements are clear and will issue appropriate additional guidance as necessary.

69. In circumstances in which commercial information is required to be submitted to the government, the Commission, consistent with statute, may withhold such records where release would likely cause substantial harm to the competitive position of the submitting party.[107] The Commission's rules explicitly list certain types of materials in the category of trade secrets and commercial and financial information that are automatically afforded certain degrees of protection from public inspection.[108] As a general matter, the harm must flow from affirmative use of the information by competitors and not consist solely of injuries that flow from customer disgruntlement or public embarrassment.[109] We also are obliged to consider any adverse impact that disclosure might have on government programs, including the impact on the Commission's ability to implement its statutory responsibility under the Communications Act.[110]

70. We agree with TIA and Motorola that information on how software within a software defined radio operates would be company proprietary information and that making this information publicly available would result in competitive harm to a manufacturer. Further, we find that information

---

[105] *See* 47 C.F.R. § 2.1033(b)(4) and (b)(5).

[106] A state description is the current or last known status of a process, such as a software routine in a radio.

[107] *See* 5 U.S.C. § 552(b) (4) (under exemption 4 of the Freedom of Information Act, agencies may withhold "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential"). *See* also Critical Mass Energy Project v. NRC, 975 F.2d 871, 880 (D.C. Cir. 1992) (en banc); National Parks & Cons. Ass'n v. Morton, 498 F.2d 765 (D.C. Cir. 1974).

[108] *See* 47 C.F.R. § 0.457(d)(1).

[109] *See, e.g.,* CNA Fin. Corp. v. Donovan, 830 F.2d 1132, 1152, 1154 & n.158 (D.C. Cir. 1987); Public Citizen Health Research Group v. FDA, 704 F.2d 1280, 1291 n.30 (D.C. Cir. 1983); Gen. Elec. Co. v. NRC, 750 F.2d 1394, 1402 (7th Cir. 1984); Center to Prevent Handgun Violence v. United States Dep't of the Treasury, 981 F. Supp. 20, 23 (D.D.C. 1997).

[110] *See, e.g.,* Critical Mass, 975 F.2d at 879 (recognizing third, program impairment prong of exemption 4); 9 to 5 Org. for Women Workers v. Bd. Of Governors of the Fed. Reserve Sys., 721 F.2d 1, 10 (1st Cir. 1983); Pub. Citizen Health Research Group v. NIH, 209 F. Supp. 2d 37, 42-43 (D.D.C. 2002) (alternative holding); Allnet Comm. Srvs. V. FCC, 800 F. Supp. 984, 990 (D.D.C. 1992).

on the security methods that manufacturers employ to prevent unauthorized modifications to the RF operating parameters of a device would be considered company proprietary information. Additionally, making information on security measures publicly available could assist unauthorized parties in determining ways to defeat them. We also conclude that, if we were to make information on software defined radio operation and security measures generally available to the public, entities seeking equipment certification may not provide sufficient information for the Commission to determine whether the device at issue would operate in compliance with our rules. Accordingly, we will modify Section 0.457(d) of the rules to state that the descriptions of the security features and software operation for a software defined radio are presumptively protected from public disclosure and will not routinely be made available for public inspection. This presumptive protection will apply only to the descriptions of the security features and software operation for a software defined radio and not to any other exhibits in the application for certification which will normally be made available for public inspection after grant of the application. An applicant for certification of a software defined radio must file a specific request and pay the appropriate filing fee to have other exhibits in the application held confidential, assuming the exhibits are eligible for confidential treatment. To avoid possible delays in processing applications, applicants should ensure that exhibits for which confidential treatment is automatically afforded or for which it is requested are clearly identified and that these exhibits do not contain information that is not eligible for such treatment.

71. We decline to allow TCBs to certify software defined radios at this time. The changes that we are adopting to automatically afford confidential treatment to the description of software and security features in software defined radio applications address the confidentiality concerns of parties who requested that TCBs be allowed to certify software defined radios to protect this information from public disclosure. Additionally, as the Commission has previously stated, because software defined radio is a new technology, TCBs will not be permitted to certify software defined radios until the Commission has more experience with them and can properly advise TCBs on how to apply the applicable rules.[111] The Commission's Laboratory maintains a list of types of devices, including software defined radios, that TCBs are excluded from certifying. The Laboratory will remove software defined radios from this exclusion list when it determines that TCBs are capable of certifying them.

3. Automatic frequency selection by unlicensed devices

72. We are changing Part 15 of the rules to allow certification of unlicensed transmitters that are capable of operation outside of permissible Part 15 frequency bands, provided the transmitters incorporate an automatic frequency selection mechanism to ensure that they operate only on frequencies where unlicensed operation is permitted when operated in the United States.

73. Many frequency bands where unlicensed operation is permitted are not harmonized worldwide.[112] Unlicensed transmitters are now being manufactured in which the frequency range of operation is software selectable to allow operation in multiple countries. However, a transmitter cannot

---

[111] *See First Report and Order* in ET Docket No. 00-47, 16 FCC Rcd 17373 (2001).

[112] For example, in the United States, unlicensed operation is permitted in the 2400-2483.5 MHz portion of the 2400-2500 MHz ISM band. The 2483.5-2500 MHz portion of this ISM band is used for the Mobile Satellite Service (MSS) in the United States and is a restricted band under Part 15 of the rules. Unlicensed devices are not permitted to transmit in that band in the United States to prevent interference to the MSS, while in other countries unlicensed operation is permitted in all or part of the 2483.5-2500 MHz band. *See* 47 C.F.R. §§ 15.205, 15.247, 15.249 and 25.202.

be approved in the United States unless it is capable of complying with the technical requirements of the rule part under which it will be operated.[113] Therefore, an unlicensed transmitter that is capable of operation outside permissible bands of operation under Part 15 of the rules cannot be certified for operation in the United States. Manufacturers would like the ability to certify devices to operate over a wider frequency range than is permissible in the United States, but incorporate technology that selects the appropriate operating frequency ranges based on the country in which they are used. A device could limit its operation to permissible frequencies when used in the United States, but could operate on additional frequencies as permitted in other countries. This approach could allow the production of devices that could be used worldwide, or at least in a number of different countries, and eliminate the need for manufacturers to produce multiple versions of a device for use in different countries.

74. In the *Notice*, we proposed to allow certification of Part 15 devices that are capable of operating on non-Part 15 frequencies to benefit consumers and manufacturers by reducing production costs and allowing production of devices that can be used in both the United States and other countries.[114] We proposed to require that such devices incorporate a method to determine the country of operation and select the appropriate operating frequency range, which must be limited to permissible Part 15 frequencies when the device is used in the United States.[115]

75. Several parties support the proposals to allow frequency selectable devices and recommend that the Commission allow the use of the IEEE 802.11d feature for enabling/disabling transmissions in certain bands.[116] The Wi-Fi Alliance states that the IEEE 802.11d feature uses a master/client scheme similar to multi-band mobile phones where a signal from the controller indicates the proper channels to the client devices.[117] The Wi-Fi Alliance, ITI and Dell recommend that the Commission limit the certification of access points[118] to the frequency range permitted in the United States.[119] Several parties

---

[113] *See* 47 C.F.R. § 2.915(a)(1).

[114] *See Notice* at 26895.

[115] *Id.*

[116] *See* Wi-Fi Alliance comments at 7, ITI comments at 10, Cisco comments at 15 and Dell comments at 5.

[117] *See* Wi-Fi Alliance comments at 7. The IEEE 802.11 Task Group d (TGd) developed IEEE Std 802.11d-2001, which is an amendment to IEEE Std 802.11, 1999 Edition. The 802.11d standard describes specifications for operation of wireless LANs in different regulatory domains, e.g., different countries. According to this standard, a wireless LAN can transmit a data string that includes a code that identifies the country of operation and allows devices in a system to configure their operation to the parameters permitted in that country. When a device that is enabled for operation across regulatory domains commences operation, it passively scans to locate at least one valid channel upon which it detects IEEE Std 802.11 data frames. The frames contain information on the country, maximum allowable transmit power and permitted channels of operation. The device can then send out a request on an authorized channel for any additional regulatory information that it has not yet received.

[118] An access point is a transceiver that operates either as a bridge in a peer-to-peer connection or as a connector between the wired and wireless segments of the network. The Commission's rules define access point in the context of the U-NII rules, but the term is also commonly used for devices that operate under other rule parts. *See* 47 C.F.R. § 15.403(a).

[119] *See* Wi-Fi Alliance comments at 7, ITI comments at 10 and Dell comments at 5.

believe that allowing an individual end user to configure a master/client system would create an unnecessary risk that a device would be deployed on an unauthorized frequency, but support giving the ability to configure a system to a system installer in an enterprise or service provider environment.[120] Intel states that devices operating under the control of a master controller should be exempted from DFS or other requirements, which would be consistent with the U-NII proceeding and allow devices to be manufactured much more economically while not sacrificing interference protection.[121]

76. The Society for Broadcast Engineers opposes allowing the importation and marketing of devices that are capable of operating in the 2483.5-2500 MHz band because they may cause interference to grandfathered broadcast auxiliary service stations that operate in this band.[122] It states that the need for a device to be able to determine the country it is located in would likely increase the cost of the device beyond that practical for a mass produced, low cost Part 15 device, and there would be a strong incentive to defeat the 2483.5-2500 MHz frequency lock out.[123]

77. We will allow certification of Part 15 devices that operate outside permissible frequency bands using a master/client model. The terms "master" and "client" were defined in the U-NII proceeding for U-NII devices.[124] We will define these terms for other types of Part 15 devices consistent with the U-NII definitions. That is, a master device will be defined as a device operating in a mode in which it has the capability to transmit without receiving an enabling signal. In this mode it is able to select a channel and initiate a network by sending enabling signals to other devices. A network always has at least one device operating in master mode. A client device will be defined as a device operating in a mode in which the transmissions of the device are under control of the master. A device in client mode is not able to initiate a network. We, of course, require master devices marketed within the United States to operate only in permissible Part 15 frequency bands, which will ensure that they enable operation of client devices only within permissible Part 15 frequency bands. Manufacturers that wish to market master devices that are hardware-capable of operating outside of permissible Part 15 frequency bands for use in other countries, but use software to limit their operation to permissible Part 15 frequency bands, must incorporate security features into them to limit the operating frequency range for devices marketed in the United States and must certify the devices as software defined radios. Different software can then be installed in master devices that are used outside of the United States to change the operating frequency range for use in other countries. Client devices that can also act as master devices must meet the certification requirements of a master device, and thus must be certified as software defined radios if the manufacturer wishes to incorporate additional frequency bands for use in other countries.

78. We will allow the certification of client devices such as wireless LAN cards used in desktop or notebook computers if they have the capability of operating outside permissible Part 15 frequency

---

[120] *See* ITI comments at 9, Dell comments at 4, Cisco comments at 15 and TIA comments at 9.

[121] *Id.*

[122] *See* SBE comments at 4.

[123] *See* SBE comments at 4-5.

[124] *See Report and Order* in ET Docket No. 03-122, 18 FCC Rcd 24484 (2003) at Appendix C.

bands.[125] As defined above, client devices may transmit only under the control of a master device. Because master devices are limited to operation on permissible Part 15 frequencies, they will direct client devices to operate on only permissible Part 15 frequencies.

79. The changes we are adopting will benefit manufacturers by allowing production of devices that can be used in multiple countries, thus reducing equipment costs.[126] At the same time, the requirement to limit the frequency range of master devices sold in the United States will minimize the likelihood that devices will operate outside permissible frequency bands and cause interference to authorized services.

C. Interruptible Spectrum Leasing

80. In this section, we are describing the technical methods that a cognitive radio could use to enable interruptible secondary use of licensed spectrum by other parties. The concepts in this section would apply to lessors who want a high level assurance of reclaiming leased spectrum when they need it.

81. In the *Notice*, we sought comment on how cognitive radios could enable secondary markets in licensed spectrum. We described two general categories of access and reversion mechanisms that could be used by a lessee to gain access to spectrum on a secondary basis and allow the spectrum to revert back to the primary licensee when necessary.[127] One category relies on the overt permission of the licensee and the other relies on equipment that senses the spectrum operating environment.[128]

82. A particular access/reversion mechanism described in the *Notice* that relies on the overt permission of the licensee is a "beacon" that can enable leased spectrum. Under this approach, use can be interrupted quickly with a high degree of reliability.[129] In a beacon system, the lessee's transmitter must have the ability to receive a control signal sent continuously by the licensee at times when transmissions by the lessee are permitted. The lessee may not commence transmissions if the beacon signal is not received, and if the beacon signal is present but then stops while the lessee is transmitting, transmissions must cease within a specified time interval. The beacon could be an RF signal sent by the licensee on a designated control frequency, or it may be a signal received over a physical connection such as fiber, copper or coaxial cable. If the beacon signal suffers from unfavorable propagation or the physical connection is lost, the licensee has "fail-safe" protection against interference, because if the lessee cannot hear the beacon signal, it must cease transmission.

83. Another mechanism that relies on the overt permission of the licensee involves a "handshaking" approach. This would offer more reliability and security by requiring the lessee to receive explicit permission to use spectrum before each transmission. However, implementation of a

---

[125] Note, however, that devices such as LAN cards that can function in master mode in networks like mesh networks, and in master mode can enable clients or peers to function outside authorized Part 15 frequencies, must be certified as master devices.

[126] The ability of a manufacturer to sell equipment in other countries would, of course, be determined by relevant regulatory authorities in those countries.

[127] *See Notice* at 26880.

[128] *Id.*

[129] *Id.*

handshaking approach may increase the complexity of implementation. Other examples of access/reversion mechanisms that rely on the overt permission of a licensee include one that would allow a lessee to transmit until the licensee signals the user to cease operation. The reliability of this approach is limited because a lessee who is unable to hear the signal ordering it to cease operation may not be aware that it should relinquish use of the spectrum.

84. In the *Notice*, we sought comment on possible regulatory approaches for the use of the beacon model or other access/reversion mechanisms for interruptible spectrum leasing. One approach would be to establish a technical model for reliable access to and secure reversion of leased spectrum that certain licensees would have the option of using to structure their leasing arrangements. Another would be for the Commission to adopt the technical model in the form of rules for lessees of spectrum. We stated that under either approach, the establishment of technical criteria for cognitive radio devices to provide access/reversion of leased spectrum could help to achieve the significant benefits of spectrum leasing without detrimentally affecting licensees' ability to access spectrum.

85. Although there was interest in the availability of interruptible spectrum leasing,[130] parties did not address the specific technical mechanisms we set out in the *Notice*. Several parties generally express concern about the technical viability of interruptible spectrum leasing.[131] However, two of these parties claim that interruptible leasing may be practical on trunked systems, which have a centralized system control.[132] Other parties believe that cognitive based leasing mechanisms such as beacon networks are possible, but worry that they would result in high leasing costs.[133] No party suggested that it would be helpful at this point for the Commission to adopt a particular technical model for interruptible spectrum leasing.

86. As described below, we find that there are technologies available now or under development that could safely allow for interruptible spectrum leasing. We find that cognitive radio technologies, or even trunked radio technologies, would allow implementation of the following general principles that interested parties state would be essential to enable interruptible leased use of spectrum:

1. The licensee must have positive control as to when the lessee can access the spectrum.

2. The licensee must have positive control to terminate the use of the spectrum by the lessee so it can revert back to the licensee's use.

3. Reversion must occur immediately upon action by the licensee unless that licensee has made specific provisions for a slower reversion time.

4. The equipment used by the licensee and the lessee must perform access and reversion functions with an extremely high degree of reliability.

---

[130] *See* St. Clair County *ex parte* submission received July 23, 2004.

[131] *See* New York State Office for Technology reply comments at 3, APCO comments at 4 and Motorola comments at 15.

[132] *See* New York State Office for Technology reply comments at 3 and APCO comments at 4.

[133] *See* Ericsson comments at 8 and Nokia comments at 4.

5. The equipment used by the licensee and the lessee must incorporate security features to prevent inadvertent misuse of, and to thwart malicious misuse of, the licensee's spectrum.

87. There are at least three different technical approaches that currently exist or are under development that a licensee could employ that would comply with the intent of these principles and enable interruptible spectrum leasing. One approach would be for a licensee to allow leasing using an existing trunked system. A trunked system uses a central controller to select the operating frequencies of radios in the system. When a radio is ready to begin transmitting, it sends a request for an operating frequency to a central controller over a control channel. The controller dynamically assigns an operating frequency to that radio and the other radios with which it communicates. Such a centralized system could be used to assign channels to radios operating under the terms of a lease, or de-assign channels when a licensee needs to use the spectrum. This could be done through a wireless control channel as is currently done to assign channels to radios in the system. Alternatively, information about leased channel availability could be provided by the trunked system controller to the lessee's equipment through a wired link.

88. The beacon approach proposed in the *Notice* and described above is similar to a trunked system in that it uses a centralized controller to enable operation of lessee's equipment. The beacon could operate either on a frequency licensed to the public safety entity or on a separate control frequency in another band. The approach would require additional infrastructure such as the beacon transmitters and radios that are capable receiving the beacon and adjusting their operation in response to the beacon signal.

89. A third method that could enable leased use of spectrum is by an exchange of "tokens" sent to the lessee's devices. Token approaches rely on the encrypted exchange of unique information to verify a user's identity when opening and maintaining a secure communications exchange. Tokens would provide a means of ensuring that lessees transmit only on available frequencies when they receive an electronic token authorizing them to do so. These tokens could also enforce terms of a lease such as the specific period of time that transmission on a frequency is allowed, thus providing a licensee with a high level of confidence that lessees will vacate the spectrum when required under the terms of the lease. Such token technology is already in use in other resource allocation problems, such as the enforcement of software license terms and avoiding data transmission conflicts between computers on local area networks.[134]

90. At this point, we see no need to adopt any particular technical model for interruptible spectrum leasing. Ultimately, a licensee must itself be satisfied that the technical mechanism being implemented under a lease does in fact provide it with the ability in real time to reclaim use of its spectrum when necessary.

---

[134] Token ring networks send an electronic message (a token) successively to each computer in the network. To avoid conflicts, a computer is permitted to send data only when it has received the token. If a computer has no data to send, it passes the token to the next computer in the network. Each computer may hold the token for only a limited amount of time. Token ring networks were developed in the 1970's and are addressed in the IEEE 802.5 standard.

IV. PROCEDURAL MATTERS

91. *Final Regulatory Flexibility Analysis.* The Final Regulatory Flexibility Analysis for this Report and Order, pursuant to the Regulatory Flexibility Act, *see* 5 U.S.C. § 604, is contained in Appendix C.

92. This document contains modified information collection requirements subject to the Paperwork Reduction Act of 1995 (PRA), Public Law 104-13. It will be submitted to the Office of Management and Budget (OMB) for review under Section 3507(d) of the PRA. OMB, the general public, and other Federal agencies are invited to comment on the new or modified information collection requirements contained in this proceeding. In addition, we note that pursuant to the Small Business Paperwork Relief Act of 2002, Public Law 107-198, *see* 44 U.S.C. 3506(c)(4), we previously sought specific comment on how the Commission might "further reduce the information collection burden for small business concerns with fewer than 25 employees."

93. In this present document, we have assessed the effects of requiring certain devices to contain security features and be certified as software defined radios and of requiring a software description in place of software source code at the time of product certification. We find that these changes would affect all businesses equally regardless of size.

94. For further information regarding this Report and Order, contact Mr. Hugh L. Van Tuyl, Office of Engineering and Technology, (202) 418-7506, e-mail Hugh.VanTuyl@fcc.gov.

V. ORDERING CLAUSES

95. Accordingly, IT IS ORDERED that pursuant to the authority contained in Sections 4(i), 301, 302, 303(e), 303(f) and 303(r) of the Communications Act of 1934, as amended, 47 USC Sections 154(i), 301, 302, 303(e), 303(f) and 303(r), this Report and Order IS ADOPTED and Parts 0, 2 and 15 of the Commission's Rules ARE AMENDED as set forth in Appendix A effective 90 days after publication in the Federal Register.

96. IT IS FURTHER ORDERED that the Commission's Consumer and Governmental Affairs Bureau, Reference Information Center, SHALL SEND a copy of this Report and Order, including the Final Regulatory Flexibility Analysis in Appendix C, to the Chief Counsel for Advocacy of the Small Business Administration.

FEDERAL COMMUNICATIONS COMMISSION

Marlene H. Dortch
Secretary

APPENDIX A: FINAL RULE CHANGES

Part 0 of Title 47 the Code of Federal Regulations is amended as follows:

1. The authority citation for Part 0 continues to read as follows:

    AUTHORITY: Secs. 5, 48 Stat. 1068, as amended; 47 U.S.C. 155.

2. Section 0.457 is amended by appending the following text to paragraph (d)(1)(ii)

§ 0.457 Records not routinely available for public inspection.

* * * * *
(d) * * *
(1) * * *
(ii) * * *Portions of applications for equipment certification of software defined radios that describe the operation of the device's software and security features will not be made available for inspection.
* * * * *

Part 2 of Title 47 of the Code of Federal Regulations is amended as follows:

3. The authority citation for Part 2 continues to read as follows:

AUTHORITY: 47 U.S.C. 154, 302a, 303 and 336, unless otherwise noted.

Section 2.1 is revised by changing the following definition:

4. § 2.1 Terms and definitions.

* * * * *
(c) * * *
Software defined radio. A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.
* * * * *

5. Section 2.932 is revised by removing paragraph (e).

6. Section 2.944 is revised to read as follows:

§ 2.944 Software defined radios.

(a) Manufacturers must take steps to ensure that only software that has been approved with a software defined radio can be loaded into the radio. The software must not allow the user to operate the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved. Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can

be legally loaded into a device to meet these requirements and must describe the methods in their application for equipment authorization.

(b) Any radio in which the software is designed or expected to be modified by a party other than the manufacturer and would affect the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, must comply with the requirements in paragraph (a) of this section and must be certified as a software defined radio.

(c) Applications for certification of software defined radios must include a high level operational description or flow diagram of the software that controls the radio frequency operating parameters.

7. Section 2.1033 is revised by adding new paragraphs (b)(12) and (c)(18) to read as follows:

§ 2.1033 Application for certification.

* * * * *

(b) * * *

(12) An application for certification of a software defined radio must include the information required by §2.944.

* * * * *

(c) * * *

(18) An application for certification of a software defined radio must include the information required by §2.944.

* * * * *

Section 2.1043 is amended by revising paragraph (b)(3) to read as follows:

§ 2.1043 Changes in certificated equipment.

* * * * *

(b)* * *

(3) A Class III permissive change includes modifications to the software of a software defined radio transmitter that change the frequency range, modulation type or maximum output power (either radiated or conducted) outside the parameters previously approved, or that change the circumstances under which the transmitter operates in accordance with Commission rules. When a Class III permissive change is made, the grantee shall supply the Commission with a description of the changes and test results showing that the equipment complies with the applicable rules with the new software loaded, including compliance with the applicable RF exposure requirements. The modified software shall not be loaded into the equipment, and the equipment shall not be marketed with the modified software under the existing grant of certification, prior to acknowledgement by the Commission that the change is

acceptable. Class III changes are permitted only for equipment in which no Class II changes have been made from the originally approved device.

NOTE TO PARAGRAPH (b)(3):
Any software change that degrades spurious and out-of-band emissions previously reported to the Commission at the time of initial certification would be considered a change in frequency or modulation and would require a Class III permissive change or new equipment authorization application.

* * * * *

Part 15 of Title 47 of the Code of Federal Regulations is amended as follows:

8. The authority citation of Part 15 continues to read as follows:

AUTHORITY: 47 U.S.C. 154, 302, 303, 304, 307, 336, and 544A.

9. A new Section 15.202 is added to read as follows:

§ 15.202 Certified operating frequency range

Client devices that operate in a master/client network may be certified if they have the capability of operating outside permissible Part 15 frequency bands, provided they operate on only permissible Part 15 frequencies under the control of the master device with which they communicate. Master devices marketed within the United States must be limited to operation on permissible Part 15 frequencies. Client devices that can also act as master devices must meet the requirements of a master device. For the purposes of this section, a master device is defined as a device operating in a mode in which it has the capability to transmit without receiving an enabling signal. In this mode it is able to select a channel and initiate a network by sending enabling signals to other devices. A network always has at least one device operating in master mode. A client device is defined as a device operating in a mode in which the transmissions of the device are under control of the master. A device in client mode is not able to initiate a network.

APPENDIX B: LIST OF COMMENTING PARTIES

Parties filing comments

1. Electronic Frontier Foundation
2. The Technology Companies/Center for Internet and Society
3. New York State, Office for Technology, Statewide Wireless Network
4. Mesh Networks
5. Wireless Broadband Operators Coalition
6. The Wi-Fi Alliance
7. IEEE USA
8. IEEE 802
9. Data Flow Systems, Inc.
10. Tucson Amateur Packet Radio Corporation
11. Vanu, Inc.
12. Itron, Inc.
13. National Public Safety Telecommunications Council
14. Information Technology Industry Council
15. Shared Spectrum Company
16. Motorola, Inc.
17. Cingular Wireless LLC and BellSouth Corporation
18. Public Knowledge and Consumers Union
19. Cisco Systems, Inc.
20. Ericsson Inc
21. Sirius Satellite Radio Inc. and XM Radio Inc.
22. Eli Sheffer
23. Cellular Telecommunications & Internet Association
24. Globalstar, L.P. et al.
25. Telecommunications Industry Association
26. Verizon Wireless
27. Association of Public-Safety Communications Officials-International, Inc.
28. Nokia Inc.
29. Thomas W. Hazlett and Matthew L. Spitzer
30. Alvarion Inc.
31. Nextel Partners, Inc.
32. Wireless Communications Association International, Inc.
33. Society of Broadcast Engineers, Inc.
34. Allen Petrin
35. Raytheon
36. Access Spectrum, LLC
37. Dell
38. Pulse Link
39. Intel Corporation
40. Radio Amateur Satellite Corp.
41. SDR Forum
42. Industrial Telecommunications Association, Inc.
43. HYPRES, Inc.
44. ARRL, the National Association for Amateur Radio

45. NAS/Committee on Radio Frequencies
46. National Association of Manufacturers and MRFAC, Inc.
47. The Port Authority of New York and New Jersey
48. Texas Instruments Incorporated
49. E-ZPass Interagency Group
50. National Radio Astronomy Observatory
51. V-COMM
52. Charles Wimber
53. WaveRider Communications
54. Ken Krechmer
55. Fredric D. Letson, KC2JKQ
56. Nickolaus E. Leggett

Parties filing reply comments

1. Cornell University
2. The Technology Companies
3. IEEE 802.18
4. New York State Office for Technology
5. Shared Spectrum Company
6. V-Comm, L.L.C.
7. Verizon Wireless
8. Sprint
9. Society of Broadcast Engineers
10. AT&T Wireless Services, Inc.
11. Intel Corporation
12. Sirius Satellite Radio, Inc. and XM Radio, Inc.
13. Nextel Partners, Inc.
14. Wireless Broadband Operators Coalition
15. National Telecommunications and Information Administration

APPENDIX C: FINAL REGULATORY FLEXIBILITY ANALYSIS

As required by the Regulatory Flexibility Act (RFA),[135] an Initial Regulatory Flexibility Analysis (IRFA) was incorporated in the *Notice of Proposed Rule Making and Order, Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies (Notice).*[136] The Commission sought written public comments on the proposals in the Notice, including comment on the IRFA.[137] This Final Regulatory Flexibility Analysis conforms to the RFA.[138]

A.   Need for, and Objectives of, the Report and Order

Advances in technology are creating the potential for radio systems to use radio spectrum more intensively and more efficiently than in the past. Software-defined and cognitive, or "smart," radios are allowing and will increasingly allow more intensive access to, and use of, spectrum than possible with traditional, hardware-based radio systems. In this Report and Order, the Commission continues the process of modifying the rules to reflect these ongoing technical developments in radio technologies. The Commission first adopted rules for software defined radios in 2001, recognizing that manufacturers were beginning to use software to help determine the RF characteristics of radios, and that the equipment rules, which assumed hardware changes were needed to modify a radio's behavior, held the potential of discouraging development of software defined radios by requiring repeated approvals for repeated software changes. In light of the Commission's experience with these rules, and the record in this proceeding, it is modifying and clarifying the equipment rules to further facilitate the development and deployment of software defined and cognitive radios.

In the Report and Order, the Commission makes several changes to Parts 2 and 15 of the rules. Specifically, it:

1) eliminates the requirement for applicants and grantees of certification of software defined radios to supply a copy of the software that controls the RF operating parameters of the radio upon request
2) requires applicants for certification of software defined radios to supply a high level operational description of the software that controls the radio frequency operating parameters
3) requires that radios in which the software that controls the RF operating parameters is designed or expected to be modified by a party other than the manufacturer to incorporate a means to prevent unauthorized software changes, and requires such radios to be certified as software defined radios
4) allows certification of unlicensed transmitters that have the capability of operating outside permissible Part 15 frequency bands, provided the transmitters incorporate a software control to limit operation to permissible Part 15 frequency bands when used in the United States

---

[135] *See* 5 U.S.C. § 603. The RFA, *see* 5 U.S.C. § 601 – 612, has been amended by the Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, Title II, 110 Stat. 857 (1996).

[136] *See Notice of Proposed Rule Making and Order* in ET Docket No. 03-108, 18 FCC Rcd 26859 (2003).

[137] *Id.*

[138] *See* 5 U.S.C. § 604.

B.   **Summary of Significant Issues Raised by Public Comments in Response to the IRFA**

None.

C.   **Description and Estimate of the Number of Small Entities To Which the Rules Apply**

The RFA directs agencies to provide a description of, and, where feasible, an estimate of the number of small entities that may be affected by the proposed rules, if adopted.[139] The RFA defines the term "small entity" as having the same meaning as the terms "small business," "small organization," and "small business concern" under Section 3 of the Small Business Act.[140] Under the Small Business Act, a "small business concern" is one that: (1) is independently owned and operated; (2) is not dominant in its field of operations; and (3) meets may additional criteria established by the Small Business Administration (SBA).[141]

Wireless Communications Equipment Manufacturers

The SBA has established a small business size standard for radio and television broadcasting and wireless communications equipment manufacturing. Under this standard, firms are considered small if they have 750 or fewer employees.[142] Census Bureau data for 1997 indicate that, for that year, there were a total of 1,215 establishments[143] in this category.[144] Of those, there were 1,150 that had employment under 500, and an additional 37 that had employment of 500 to 999. The percentage of wireless equipment manufacturers in this category is approximately 61.35%,[145] so the Commission estimates that the number of wireless equipment manufacturers with employment under 500 was actually closer to 706, with and additional 23 establishments having employment of between 500 and 999. Given

---

[139] *See* U.S.C. § 603(b)(3).

[140] *Id.* § 601(3).

[141] *Id.* § 632.

[142] 1997 Economic Census, Manufacturing, Industry Series, Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing, Document No. E97M-3342B (August 1999), at 9; 1997 Economic Census, Manufacturing, Industry Series, Other Communications Equipment Manufacturing, Document No. EC97M-3342C (September 1999), at 9 (both available at http://www.census.gov/prod/www/abs/97ecmani.html).

[143] The number of "establishments" is a less helpful indicator of small business prevalence in this context than would be the number of "firms" or "companies," because the latter take into account the concept of common ownership or control. Any single physical locations for an entity is an establishment, even though that location may be owned by a different establishment. Thus, the numbers given may reflect inflated numbers of businesses in this category, including the numbers of small businesses. In this category, the Census breaks out data for firms or companies only to give the total number of such entities for 1997, which was 1,089.

[144] U.S. Census Bureau, 1997 Economic Census, Industry Series: Manufacturing, "Industry Statistics by Employment Size," Table 4, NAICS code 334220 (issued August 1999).

[145] *Id.* Table 5, "Industry Statistics by Industry and Primary Product Class Specialization: 1997."

the above, the Commission estimates that the majority of wireless communications equipment manufacturers are small businesses.

D. Description of Projected Reporting, Recordkeeping, and Other Compliance Requirements

Unlicensed transmitters are required to be certified before they can be imported into or marketed within the United States. The certification process requires the manufacturer or other party responsible for compliance to have the equipment tested and electronically file an application form, measurement report and other information on the equipment with the Commission or a designated Telecommunication Certification Body (TCB). Software defined radios at present may be approved only by the Commission and not by TCBs, although the Commission has stated that it will eventually allow TCBs to approve them. The Report and Order does not change this requirement.

Applicants for certification of a software defined radio will be required to supply a high level operational description of the software that controls the radio frequency operating parameters.

Manufacturers of radios in which the software that controls the radio frequency operating parameters is designed or expected to be modified by a party other than the manufacturer must incorporate a means to prevent unauthorized software changes that must be described in the application for certification. Such software changeable radios must be declared as software defined radios in the application for certification. Most radios at the present are not software modifiable, and manufacturers of those that are generally already take steps to prevent unauthorized modifications, so we expect that only rarely would manufacturers have to redesign equipment to comply with this requirement.

E. Steps Taken to Minimize Significant Economic Impact on Small Entities, and Significant Alternatives Considered

The RFA requires an agency to describe any significant alternatives that it has considered in reaching its proposed approach, which may include the following four alternatives (among others): (1) the establishment of differing compliance or reporting requirements or timetables that take into account the resources available to small entities; (2) the clarification, consolidation, or simplification of compliance or reporting requirements under the rule for small entities; (3) the use of performance, rather than design, standards; and (4) an exemption from coverage of the rule, or any part thereof, for small entities.[146]

The Commission sought comment in the *Notice* about whether it should make compliance with the software defined radio rules, including the requirement to demonstrate that a radio incorporates security features, mandatory rather than optional for certain types of radio transmitters. Based on the comments received, the Commission made these requirements mandatory only for the small subset of radio transmitters in which the software that controls the radio frequency operating parameters is designed or expected to be modified by a party other than the manufacturer. This change will ensure that radio transmitters can not be easily modified and cause interference to authorized services, while minimizing the filing burden on applicants for certification by requiring only a small number of devices to be certified as software defined radios.

---

[146] *See* 5 U.S.C. § 603(c).

The Commission simplified the filing requirements for software defined radios to benefit all entities, including small entities. It eliminated the requirement to supply software source code upon request because such software is not generally useful for certification review and may have become an unnecessary barrier to entry. The Commission will instead require the submission of a software description at the time of certification as supported by a number of parties in comments. Because such a description would generally be considered company proprietary information, the Commission will automatically hold such information confidential without the need for applicants for certification to file a specific request for confidentiality and pay a fee. Eliminating the need to file a specific confidentiality request and pay a fee is expected to benefit small entities that have fewer resources to comply with regulatory requirements.

Report to Congress: The Commission will send a copy of the Report and Order, including this FRFA, in a report to be sent to Congress pursuant to the Congressional Review Act, *see* 5 U.S.C. § 801(a)(1)(A). In addition, the Commission will send a copy of the Report and Order, including FRFA, to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the Report and Order and FRFA (or summaries thereof) will also be published in the Federal Register. *See* 5 U.S.C. § 604(b).

STATEMENT OF
COMMISSIONER JONATHAN S. ADELSTEIN

Re: *Facilitating Opportunities for Flexible, Efficient, and Reliable Spectrum Use Employing Cognitive Radio Technologies ET Docket No. 03-108; Report and Order*

I've been fortunate to be involved in our work on cognitive radio technologies since helping the Office of Engineering and Technology open its workshop on cognitive radio technologies in the spring of 2003. I remarked then that cognitive radios could play a key role in shaping our spectrum use in the future. As we see in our item today, the enormous potential of cognitive radios is being realized increasingly every day. I very much appreciate the effort of OET and others in pushing this forward – making sure our rules keep pace with this cutting edge technology.

I believe that cognitive radios will play an important role in "spectrum facilitation." That means stripping away barriers – regulatory, economic, or technical – to get spectrum into the hands of operators serving consumers at the most local levels. Cognitive radios can literally leapfrog the technical and legal problems that currently hamper many of today's spectrum access opportunities. Spectrum policy is a two-sided coin: a framework for innovation on one side, with spectrum facilitation on the other.

These technologies should lead to the advent of smarter unlicensed devices that make greater use of spectrum than is possible today. Cognitive radios may also provide licensees with innovative ways to use their current spectrum more efficiently, and to lease their spectrum more easily on the secondary market. I've seen cognitive radios up close and am just amazed by their potential.

While we don't tackle the issue here, I remain particularly interested in our proposal from the original NPRM to allow higher power operation for unlicensed devices operating in rural and other areas of low spectrum use. I regularly hear from WISPs across the country that they need improved access to spectrum. Higher power operation can drive broadband deployment deeper and farther into all parts of America.

I also find the discussion of interruptible spectrum leasing very useful. Such a development may enable previously reluctant licensees to explore a technological fix to address some of the current challenges of spectrum leasing. It has been suggested that interruptible spectrum use could be a tool for public safety licensees should we decide to allow them to lease their spectrum to commercial providers in the future. While I remain unsure whether such a policy change is appropriate in light of our Herculean work on public safety spectrum use in the 700 and 800 MHz bands over the past couple of years, I very much appreciate the value in having a discussion on the technical aspects of interruptible spectrum leasing.

For these reasons, I enthusiastically support this item.